



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE  
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

MAIL STOP APPEAL BRIEF - PATENTS  
Commissioner for Patents  
Post Office Box 1450  
Alexandria, Virginia 22313-1450

Sir:

APPEAL BRIEF TRANSMITTAL

Enclosed herewith are three (3) copies of an Appeal Brief for this patent application together with a check in the amount of the small entity fee for filing a brief in support of an appeal.

///

///

///

///

///

///

///

///

///

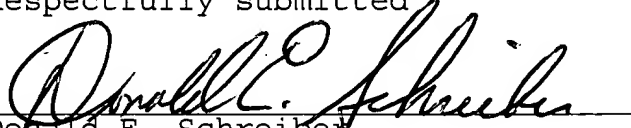
///

///

1  
Appl. No. 09/655,229  
Response Dated June 20, 2005  
Appeal of Office Action dated January 18, 2005

If any additional fee is required, the Commissioner for Patents is hereby authorized to charge any deficiency or credit any surplus in any relevant fee to Deposit Account No. 19-0735. A duplicate copy of this transmittal letter is enclosed herewith.

Respectfully submitted



Donald E. Schreiber  
Reg. No. 29,435

Dated: 20 June, 2005

Donald E. Schreiber  
A Professional Corporation  
Post Office Box 2926  
Kings Beach, CA 96143-2926

Telephone: (530) 546-6041

Attorney for Appellant



06-21-05

AF  
JW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE  
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

EV 550 280 995 US  
"Express Mail" mailing Number

20 June, 2005  
Date of Deposit

I hereby certify that this correspondence is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above addressed to:

MAIL STOP APPEAL BRIEF - PATENTS  
Commissioner for Patents  
Post Office Box 1450  
Alexandria, Virginia 22313-1450

on 20 June, 2005.

  
Donald E. Schreiber

Dated: 20 June, 2005

Donald E. Schreiber  
A Professional Corporation  
Post Office Box 2926  
Kings Beach, CA 96143-2926  
(530) 546-6041

Serial No. : 09/655,229 Confirmation No. 7777  
Appellant : Chung Nan Chang  
Filed : September 5, 2000  
Title : SECURE CRYPTOGRAPHIC KEY EXCHANGE  
AND VERIFIABLE DIGITAL SIGNATURE  
TC/A.U. : 2131  
Examiner : Shin-Hon Chen  
Docket No. : 2174  
Customer No.: 23320

MAIL STOP APPEAL BRIEF - PATENTS  
Commissioner for Patents  
Post Office Box 1450  
Alexandria, Virginia 22313-1450

Sir:

APPEAL BRIEF

Pursuant to 37 C.F.R. § 1.192, through his undersigned attorney the Appellant submits in triplicate the following brief

06/22/2005 TBESHAH1 00000013 09655229

01 FC:2402

250.00 OP

Appl. No. 09/655,229

Response Dated June 20, 2005

Appeal of Office Action dated January 18, 2005

appealing a rejection of claims that appears in an Office Action dated January 18, 2005.

### **Real Party in Interest**

The real parties in interest are:

1. the inventor, Chung Nan Chang; and
2. an assignee of fifty percent (50%) interest in the patent application, On Line Post Corp. Fl. 12, No. 123, Sec. 2, Chung Hsiao E. Road, 100 Taipei, Taiwan R.O.C.

### **Related Appeals and Interferences**

Appellant is unaware of any presently pending appeal or interference that is related to this appeal.

### **Status of the Claims**

Claims 1-29, set forth in Appendix I hereto, are pending in this application. Claims 1-29 have been finally rejected, and that rejection of claims is being appealed.

### **Status of Amendments**

Claims 1-29 are those originally filed on September 5, 2000.

Appl. No. 09/655,229  
Response Dated June 20, 2005  
Appeal of Office Action dated January 18, 2005

Summary of the Invention

Claims 1-29 include four (4) distinct categories of claims.

1. Claims 1-9 encompass a method by which cryptographic units S and R, i.e. sender and receiver, mutually establish a cryptographic key K.
2. Claims 10-18 encompass a system adapted for communicating as an encrypted cyphertext message M a plaintext message P after cryptographic units included in the system establish a cryptographic key K.
3. Claims 19-27 encompass a cryptographic unit adapted for:
  - a. inclusion in a system for communicating as an encrypted cyphertext message M a plaintext message P; and
  - b. establishing a cryptographic key K.
4. Claims 28-29 encompass a method by which a receiving unit R authenticates a sender's digital signature.

For establishing the cryptographic key K, each independent claim 1, 10 and 19 includes the following five (5) characteristic steps.

1. A receiving unit R transmits for storage in a publicly accessible repository a plurality of public quantities.<sup>1</sup>

---

<sup>1</sup> Independent claim 1 element a  
Independent claim 10 element c.i.(1)  
Independent claim 19 element a.i.(1)

Appl. No. 09/655,229

Response Dated June 20, 2005

Appeal of Office Action dated January 18, 2005

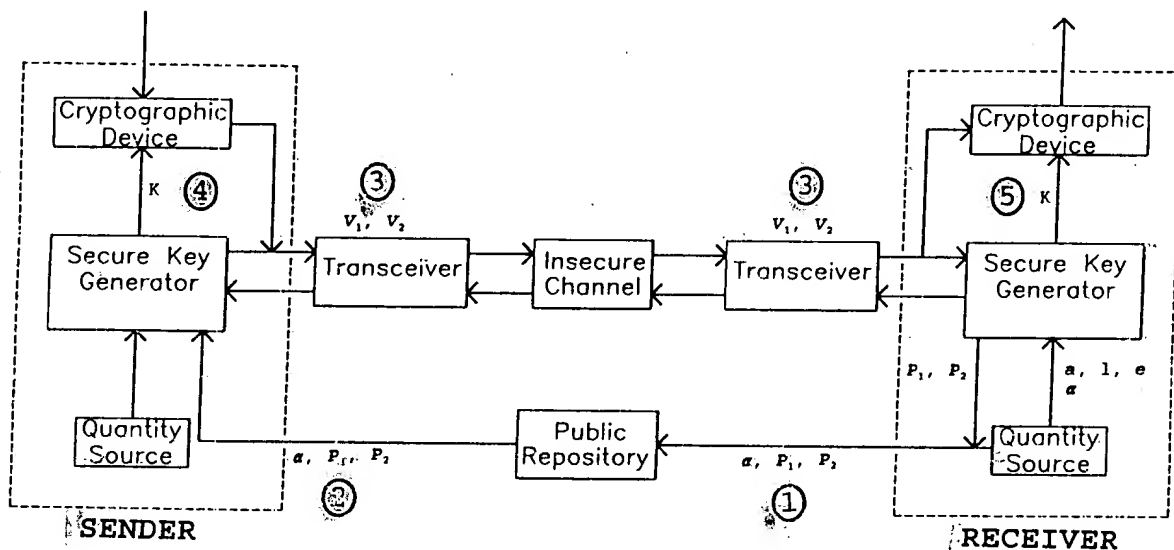
2. A sending unit S retrieves the plurality of public quantities from the publicly accessible repository.<sup>2</sup>
3. The sending unit S uses at least some of the plurality of public quantities in computing and transmitting to the receiving unit R a plurality of sender's quantities.<sup>3</sup>
4. The sending unit S uses at least one of the plurality of public quantities in computing the cryptographic key K.<sup>4</sup>
5. The receiving unit R uses at least one of the plurality of sender's quantities received from the sending unit S in computing the cryptographic key K.<sup>5</sup>

The preceding five characteristic steps, excerpted from independent claims 1, 10 and 19, clearly encompass only establishing a cryptographic key K by both sender and receiver. Accordingly, the preceding five characteristic steps do not encompass transmitting either:

- 
- |   |                                       |
|---|---------------------------------------|
| 2 | Independent claim 1 element b.i       |
|   | Independent claim 10 element c.ii     |
|   | Independent claim 19 element a.ii     |
| 3 | Independent claim 1 element b.ii      |
|   | Independent claim 10 element c.ii.(1) |
|   | Independent claim 19 element a.ii.(1) |
| 4 | Independent claim 1 element b.iii     |
|   | Independent claim 10 element c.ii.(2) |
|   | Independent claim 19 element a.ii.(2) |
| 5 | Independent claim 1 element c.        |
|   | Independent claim 10 element c.i.(2)  |
|   | Independent claim 19 element a.i.(2)  |

1. an encrypted plaintext, i.e. a cyphertext; or
2. a digital signature.

The following diagram, an annotated, redacted copy of the patent application's FIG. 1, graphically illustrates common characteristic steps 1-5 summarized above in the context of the patent application's detailed description.



As illustrated above:

1. the receiver, enclosed within the dashed box at the right hand side of the preceding illustration, transmits for storage in the public repository the plurality of quantities:
  - a.  $\alpha$  generated by the quantity source<sup>6</sup>; and

<sup>6</sup> See the pending application at page 17, lines 16-19.

- b.  $P_1$  and  $P_2$  generated by the secure key generator<sup>7</sup>;
2. the sender, enclosed within the dashed box at the left hand side of the preceding illustration, retrieves the plurality of quantities  $\alpha$ ,  $P_1$  and  $P_2$  from the public repository<sup>8</sup>;
3. the sender computes and transmits to the receiver two (2) quantities  $V_1$  and  $V_2$  using at least some of the plurality of quantities  $\alpha$ ,  $P_1$  and  $P_2$  retrieved from the public repository<sup>9</sup>;
4. the sender computes the cryptographic key  $K$  using at least some of the plurality of quantities  $\alpha$ ,  $P_1$  and  $P_2$  retrieved from the public repository<sup>10</sup>; and
5. the receiver computes the cryptographic key  $K$  using at least one of the quantities  $V_1$  and  $V_2$  received from the sender<sup>11</sup>.

For authenticating a sender's digital signature, independent claim 28 requires the following steps performed by a receiving unit.

---

<sup>7</sup> See the pending application at page 18, lines 1-5.

<sup>8</sup> See the pending application at page 18, lines 12-17.

<sup>9</sup> See the pending application at page 18, line 16 to page 19, line 2.

<sup>10</sup> See the pending application at page 19, lines 9-11.

<sup>11</sup> See the pending application at page 19, lines 6-8.



Appl. No. 09/655,229

Response Dated June 20, 2005

Appeal of Office Action dated January 18, 2005

1. Retrieving a plurality of public quantities from a publicly accessible repository which the sending unit has previously stored there.
2. Using the digital signature, which the sending unit transmits together with message "M," and the plurality of public quantities, evaluating expressions of at least two (2) different verification relationships.
3. Comparing pairs of results obtained by evaluating the expressions of the at least two (2) different verification relationships.

#### The Issues

1. Whether method, system and cryptographic unit claims 1-27 are anticipated under 35 U.S.C. § 102(b) by United States Patent No. 5,804,703 entitled "Method and Apparatus for Digital Signature Authentication" which issued September 8, 1998, on an application filed by Richard E. Crandall ("the Crandall patent").
2. Whether digital signature claims 28 and 29 are anticipated under 35 U.S.C. § 102(b) by the Crandall patent.

Appl. No. 09/655,229  
Response Dated June 20, 2005  
Appeal of Office Action dated January 18, 2005

### Claim Groups

Claims 1-27's rejections under 35 U.S.C. § 102(b) stand or fall by together.

Claims 28 and 29 rejections under 35 U.S.C. § 102(b) stand or fall by together.

### Argument

First, this patent application's prosecution history contains irrefutable proof that Appellant's communications either have not been read, or have not been understood.

For example, a March 28, 2005, Advisory Action<sup>12</sup> contains the following statement.

Regarding to applicant's arguments, applicant argues that the storage of any information or data into the public source either by a sender or by a receiver is not disclosed in the Crandall reference in its text or implicitly. However, Crandall discloses the public source contains the public keys of the sender and receiver, which inherently discloses that the public keys are transmitted by the sender and receiver (Crandall. column 20 lines 15-24: the source of information may be transmitted between sender and receiver). (Emphasis supplied.)

Page 2 of the March 17, 2005, response, to which the preceding Advisory Action excerpt replies, contains the following admission by Appellant.

---

<sup>12</sup> The Advisory Action replies to a March 17, 2005, response to the final rejection of claims 1-29 appearing in a January 18, 2005, Office Action.

Appl. No. 09/655,229  
Response Dated June 20, 2005  
Appeal of Office Action dated January 18, 2005

Specifically, the Applicant finds that the "public source 813" disclosed in the cited reference receives, either expressly or implicitly:

1. only ourPub from a sender; and
2. only theirPub from a receiver.

Since the preceding excerpt from the March 17, 2005, response to the January 18, 2005, Office Action's final rejection of claims 1-29 expressly contradicts the statement excerpted above from the March 28, 2005, Advisory Action, clearly Appellant's communications either have not been read, or have not been understood.

#### The Cited Reference

Proceeding now to the substance of the January 18, 2005, Office Action's final rejection of claims 1-27, the Crandall patent discloses that:

[i]n the following description, the terms "our" and "our end" refer to the sender. The terms "their" and "their end" refer to the receiver. This convention is used because the key exchange of the present invention may be accomplished between one or more senders and one or more receivers. Thus, "our" and "our end" and "their" and "their end" refers to one or more senders and receivers, respectively.

The public key exchange of the elliptic curve cryptosystem of the present invention is illustrated in the flow diagram of FIG. 3.

Step 301

At our end, a public key is computed:  $\text{ourPub} \in F_{pk}$

$$\text{ourPub} = (\text{ourPri})^o(x_1, y_1) \quad \text{Equation (12)}$$

Step 302

At their end, a public key is computed:  $\text{theirPub} \in F_{pk}$

$$\text{theirPub} = (\text{theirPri})^o(x_1, y_1) \quad \text{Equation (13)}$$

Step 303

The two public keys ourPub and theirPub are published, and therefore known to all users. (Col. 8, lines 1-23) (Emphasis supplied.)

A separate source 813<sup>13</sup> stores publicly known information, such as the public keys "ourPub" and "theirPub" of sender 801 and receiver 802, the initial point  $(x_1, y_1)$ , the field  $F_{pk}$ , and curve parameter "a". This [public] source [813] of information may be a published directory, an on-line source for use by computer systems, or it[, i.e. the public source 813,] may transmitted between sender and receiver over a non-secure transmission medium. The public source 813 is shown symbolically connected to sender 801 through line 815 and to receiver 802 through line 814.<sup>14</sup>

In operation, the sender and receiver generate a common one time pad for use as an enciphering and deciphering key in a secure transmission. The private key of the sender, ourPri, is provided to the elliptic multiplier 805, along with the sender's public key, theirPub<sup>15</sup>. The elliptic multiplier 805 computes an enciphering key  $e_k$  from  $(\text{ourPri})^o(\text{theirPub}) \pmod{p}$ . (Col. 13, lines 9-24.) (Emphasis supplied.)

---

<sup>13</sup> Depicted both in FIG. 8 and in FIG. 12. "FIG. 8 is a block diagram of the present invention." (Col. 12, line 51.) "FIG. 12 illustrates a block diagram for implementing the digital signature scheme of the present invention." (Col. 19, lines 34-35.)

<sup>14</sup> Note that lines 814 and 815, both in FIGs. 8 and 12, in all instances terminate in arrows that are directed away from rather than toward the public key source 813. Thus, FIGs. 8 and 12 teach away from storage of information or data either by the sender 801 or 1201 or by the receiver 802 or 1202 into the "public source 813." Consequently, the only disclosure of information or data storage into the "public source 813" by either the sender 801 or 1201 or by the receiver 802 or 1202 must reside in the text of the Crandall patent.

<sup>15</sup> It appears that this text should correctly read "along with the ~~sender's~~ receiver's public key, theirPub."

The receiver 802 generates a deciphering key  $D_k$  using the receiver's private key, theirPri. TheirPri is provided from the private key source 808 to the elliptic multiplier 804, along with sender's public key, ourPub, (from the public source 813). Deciphering key  $D_k$  is generated from  $(\text{theirPri})^\circ(\text{ourPub}) \pmod{p}$ . The deciphering key  $D_k$  is equal to the enciphering key  $e_k$  due to the abelian nature of the elliptic multiplication function. Therefore, the receiver 802 reverses the encryption scheme, using the deciphering key  $D_k$ , to recover the plaintext message Ptxt from the ciphertext message C. (Col. 13, lines 31-40.) (Emphasis supplied.)

A separate source 813 stores publicly known information, such as the public keys "ourPub" and "theirPub" of sender 1201 and receiver 1202, the initial point  $(x_1, y_1)$ , the field  $F_{pk}$ , and curve parameter "a". This source of information may be a published directory, an on-line source for use by computer systems, or it may be transmitted between sender and receiver over a non-secure transmission medium. The public source 813 is shown symbolically connected to sender 1201 through line 815 and to receiver 1202 and hasher 1206 through lines 814 and 1218 respectively.

In operation, the sender and receiver generate a common one time pad for use as an enciphering and deciphering key in a secure transmission, as described above. (Col. 20, lines 15-27.) (Emphasis supplied.)

The receiver 1202 generates a deciphering key  $D_k$  using the receiver's private key, theirPri. TheirPri is provided from the private key source 808 to the elliptic multiplier 806, along with sender's public key, ourPub, (from the public source 813). Deciphering key  $D_k$  is generated from  $(\text{theirPri})^\circ(\text{ourPub}) \pmod{p}$ . The deciphering key  $D_k$  is equal to the enciphering key  $e_k$  due to the abelian nature of the elliptic multiplication function. Therefore, the receiver 1202 reverses the encryption scheme, using the deciphering key  $D_k$ , to recover the plaintext message from the ciphertext message C.

The elliptic multiplier 806 of the receiver 1202 receives point u from the nonsecure channel 816. The elliptic multiplier (sic) 806 generates point Q and provides it to comparator 1208. Hasher receives (sic) the ciphertext message C and point P from the nonsecure channel 816 and the purported sender's public key ourPub

from source 813 and generates point R, which it provides to comparator 1208. Comparator 1208 compares points Q and R and if they match, the signature is assumed to be valid. In the present invention, the comparison of points Q and R is accomplished using the optimized scheme using x values described above. (Col. 20, lines 42-63.) (Emphasis supplied.)

A redacted copy of FIG. 12 from the Crandall patent appears below that has been annotated to illustrate those portions of that reference's disclosure which correspond most nearly:

1. to the characteristic steps 1-5 identified above in independent claims 1, 10 and 19; and
2. to the annotated, redacted preceding copy of FIG. 1 from the present application.<sup>16</sup>

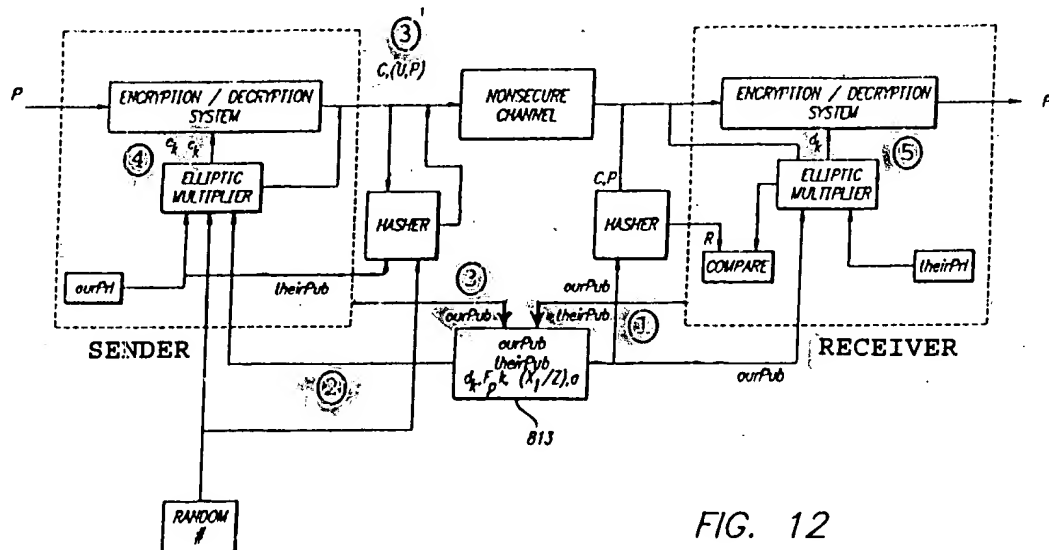


FIG. 12

<sup>16</sup> Note that in the published Crandall patent both FIG. 8 and FIG. 12 fail to graphically illustrate storage of either ourPub or theirPub into the public source 813. To rectify this apparent omission, the redacted copy of FIG. 12 from the Crandall patent includes annotations which indicate storing ourPub or theirPub into the public source 813.

As illustrated above, the Crandall patent expressly discloses only that:

1. using a public initial point ( $x_1, y_1$ ), the receiver, enclosed within the dashed box at the right hand side of the preceding illustration, computes using equation (12) and transmits for storage in the public source 813 only a single quantity theirPub<sup>17</sup>;
2. the sender, enclosed within the dashed box at the left hand side of the preceding illustration, retrieves from the public source 813 a plurality of quantities, at least:
  - a. theirPub;
  - b. the initial point ( $x_1, y_1$ ); and
  - c. a fast class number  $p$ <sup>18</sup>;
3. under one interpretation of the Crandall patent, using the public initial point ( $x_1, y_1$ ), the sender computes using equation (13) and transmits to the receiver, via the public source 813, only a single quantity ourPub<sup>19, 20</sup>; or

---

<sup>17</sup> See the Crandall patent at col. 8, lines 8-23.

<sup>18</sup> See the Crandall patent at col. 8, lines 8-23, and col. 13, lines 23-24.

<sup>19</sup> For reasons explained in greater detail below, this interpretation of the Crandall patent accords most nearly with a requirement latent in the fifth characteristic step for independent claims 1, 10 and 19.

<sup>20</sup> See the Crandall patent at col. 8, lines 8-23.

3'. under the interpretation of the Crandall patent which appears on page 3 of the January 18, 2005, Office Action, using at least the public quantities "theirPub," the initial point  $(x_1, y_1)$ , the field  $F_{pk}$ , curve parameter "a," and  $(X_1/1)$ , the sender computes and transmits to the receiver, via nonsecure channel 816:

- a. a ciphertext message C; and
  - b. a digital signature  $(u, P)^{21}$ ;
4. the sender computes, using the public quantities theirPub and p, the cryptographic key, i.e. encryption key  $e_k$ <sup>22</sup> from  $(ourPri) \circ (\text{theirPub}) \pmod p$ <sup>23</sup>; and
5. the receiver computes, using the public quantities ourPub and p, the cryptographic key K, i.e. deciphering key  $d_k$  from  $(theirPri) \circ (\text{ourPub}) \pmod p$ <sup>24</sup>.

---

<sup>21</sup> For reasons explained in greater detail below, this interpretation of the Crandall patent:

1. extends into portions of its disclosure beyond establishing a cryptographic key K; and
2. is inconsistent with a requirement latent in the fifth characteristic step for independent claims 1, 10 and 19.

<sup>22</sup> An error apparently exists in the Crandall patent's FIG. 12 where the symbol " $c_k$ " appears instead of the symbol " $e_k$ " that appears in FIG. 8. To conform this redacted, annotated copy of FIG. 12 with the text of the Crandall patent in column 20 at lines 47-49, the redacted, annotated copy of FIG. 12 includes the symbol " $e_k$ ."

<sup>23</sup> See the Crandall patent at col. 13, lines 23-24

<sup>24</sup> See the Crandall patent at col. 20, lines 46-47



A step-by-step summary, set forth below, compares the preceding analysis of the Crandall patent with characteristic steps 1-5 identified above for independent claims 1, 10 and 19.

1. The Crandall patent's text expressly discloses that the receiver transmits only a single quantity, theirPub, for storage in a publicly accessible repository, i.e. the public source 813, rather than the plurality of public quantities expressly required by the texts of independent claims 1, 10 and 19.
2. The Crandall patent correctly discloses that the sender retrieves a plurality of public quantities, i.e. theirPub, the initial point (x<sub>1</sub>, y<sub>1</sub>) and the fast class number p<sub>i</sub>, from the publicly accessible repository, i.e. the public source 813.
3. Under one interpretation, the Crandall patent's text expressly discloses that, using at least some of the plurality of public quantities, the sender computes and transmits to the receiver, via the public source 813, only a single quantity, ourPub.
- 3'. Under the interpretation that appears in the January 18, 2005, Office Action, the Crandall patent arguably discloses that, using at least some of the plurality of public quantities, the sender computes and transmits to the receiver, via the nonsecure channel 816, a plurality of sender quantities, i.e.:
  - a. the ciphertext message C; and
  - b. the digital signature (u,P).

However, pending claims 1-27 encompass only establishing a cryptographic key K. Consequently, the Office Action's interpretation of the Crandall patent relies upon portions of the reference's disclosures which extend beyond establishing the enciphering key  $e_k$  and the deciphering key  $d_k$ .

4. The Crandall patent correctly discloses that the sender uses a plurality of public quantities, i.e. theirPub and p, in computing the cryptographic key, i.e. encryption key  $e_k$ .
5. Under interpretation 3 above, the Crandall patent discloses only that the receiver uses a plurality of public quantities, i.e. ourPub and p, in computing the cryptographic key, i.e. deciphering key  $d_k$ , not a plurality of sender quantities. Interpretation 3' above, as explained in greater detail below causes the Crandall patent to disclose a cryptosystem that provides no security.

Consequently, with respect to independent claims 1, 10 and 19 as analyzed above, the Crandall patent:

1. fails to expressly disclose characteristic step 1;
2. either:
  - a. fails to disclose characteristic step 3; or
  - b. requires an interpretation which relies upon matter that is beyond the scope of claims 1-27; and
3. either:
  - a. fails to disclose characteristic step 5; or

Appl. No. 09/655,229  
Response Dated June 20, 2005  
Appeal of Office Action dated January 18, 2005

b. discloses a cryptosystem that provides no security.

**The Crandall Patent's Receiver  
Stores Only theirPub Into The  
Public Source 813**

---

In rejecting pending independent claims 1 under 35 U.S.C. § 102(b) as being anticipated by the Crandall patent, citing both column 20 at lines 15-24 and FIG. 12 in the Crandall patent the January 18, 2005, Office Action, on page 3, alleges that the Crandall patent's receiver transmits for storage "in a publicly accessible repository a plurality of public quantities."

Previously, it has been established that both FIG. 8 and FIG. 12 of the Crandall patent fail to graphically illustrate storage of anything into the publicly accessible repository. That is, all arrows in FIGs. 8 and 12 point away from the public source 813. Thus, if the Crandall patent discloses transmission for storage "in a publicly accessible repository a plurality of public quantities" as the January 18, 2005, Office Action alleges, such disclosure must occur in the Crandall patent's text, i.e. in column 20 at lines 15-24.

Set forth below is the text of the Crandall patent excerpted from column 20 at lines 15-24.

A separate **source 813** stores publicly known information, such as the public keys "**ourPub**" and "**theirPub**" of sender 1201 and receiver 1202, the initial point  $(x_1, y_1)$ , the field  $F_{pk}$ , and curve parameter "a". This source of information may be a published directory, an on-line

Appl. No. 09/655,229

Response Dated June 20, 2005

Appeal of Office Action dated January 18, 2005

source for use by computer systems, or it may be transmitted between sender and receiver over a non-secure transmission medium. The **public source 813** is shown symbolically connected to sender 1201 through line 815 and to receiver 1202 and hasher 1206 through lines 814 and 1218 respectively. (Col. 20, lines 15-24.) (Emphasis supplied.)

The preceding excerpted text clearly establishes that the public source 813 stores a plurality of public quantities. However, the preceding text fails to disclose whether the plurality of public quantities are stored in the public source 813 by:

1. the receiver;
2. the sender; or
3. a trusted third party.

The text of the Crandall patent in column 8 at lines 8-23 states only that the receiver stores theirPub into the public source 813, and that the sender stores ourPub there also. Since "for anticipation under 35 U.S.C. § 102, the reference must teach every aspect of the claimed invention either explicitly or impliedly<sup>25</sup>," because the Crandall patent explicitly discloses only the storage of theirPub and ourPub into the public source 813, the reference fails to anticipate independent claim 1 unless the receiver impliedly stores at least one quantity into the public source 813 in addition to theirPub.

---

<sup>25</sup> Manual of Patent Examining Procedure ("MPEP") Eighth Edition Revision 1, February 2003, § 706.02, p. 700-21, emphasis supplied.

Appl. No. 09/655,229  
Response Dated June 20, 2005  
Appeal of Office Action dated January 18, 2005

Regarding the possibility that the Crandall patent might "impliedly" disclose that the receiver stores into the public source 813 at least one quantity in addition to theirPub, the text of the Crandall patent in column 7 at lines 30-31 in a section of the reference entitled "Elliptic Curve Algebra" expressly states:

[N]ext, parameters are established for both sender and recipient.

The preceding excerpt from the Crandall patent expressly discloses that parameters, i.e. the public quantities present in the public source 813 in addition to theirPub and ourPub, are not established by either the sender or the recipient (receiver). Rather, the "parameters are established for both sender and recipient," presumably by some trusted third party.

Confirming this interpretation of the preceding text excerpted from column 7 of the Crandall patent, that reference in column 16, lines 15 through 22, criticizes the RSA cryptosystem because a "user cannot generate its own private key in the RSA system." Contrasting the Crandall patent's elliptic curve cryptosystem with the RSA cryptosystem, the Crandall patent in column 16 declares:

[t]he present invention does not require that the private key be a prime number. Therefore, users can generate their own private keys, so long as a public key is generated and published using correct and publicly available parameters  $p$ ,  $F_{pk}$ ,  $(X_1/Z)$  and "a".

Thus, the text in column 16 discloses that:

1. there exists cryptosystems which are so mathematically difficult that a "user" cannot generate their own private key, no less generate their own public key;
2. for such cryptosystems, a trusted third party must establish both the private and public keys; and
3. announces as a significant advance in cryptosystem technology a user's ability to select their own private key.

If a user's ability to select their own private key constitutes a significant advance in cryptosystem technology warranting specific mention, wouldn't the Crandall patent be reasonably expected to similarly expressly announce in its text a user's ability to establish the elliptic curve cryptosystem's parameters such as  $p$ ,  $F_{pk}$ ,  $(X_1/Z)$  and "a." The only reasonable inference which can be drawn from the Crandall patent's failure to specifically describe a user's ability to establish the cryptosystem's parameters is that establishing those parameters generally lies beyond a user's capability due to the mathematical complexity and difficulty of the esoteric elliptic curve cryptosystem. Consequently, the text excerpted above from column 16 confirms the statement excerpted from column 7 that the "parameters [stored in the public source 813 other than theirPub and ourPub] are established for both sender and recipient," probably by a highly mathematically-skilled, trusted third party.

Consequently, the text of the Crandall patent expressly discloses that:

1. the receiver stores only a single quantity, i.e. theirPub, into the public source 813; and
2. other quantities, i.e. the cryptosystem's parameters, are stored into the public source 813 for both sender and receiver, apparently by a trusted third party.

**Problems Inherent In The  
Crandall Patent's Alleged  
Plurality of Sender's Quantities**

In rejecting pending independent claims 1 under 35 U.S.C. § 102(b) as being anticipated by the Crandall patent, the January 18, 2005, Office Action, on page 3, citing column 13, lines 18-30 in the reference alleges that the Crandall patent's sender computes and transmits, as a plurality of sender's quantities:

1. the ciphertext message C; and
2. digital signature (u,P).

Superficially, the January 18, 2005, Office Action's selection of the ciphertext message C and digital signature (u,P) to be the "plurality of sender's quantities" required by the third characteristic step of independent claims 1, 10, and 19 may initially appear plausible. However, that interpretation of the Crandall patent, employed for rejecting independent claims 1-27, relies upon portions of the Crandall patent's disclosure which extend entirely

Appl. No. 09/655,229  
Response Dated June 20, 2005  
Appeal of Office Action dated January 18, 2005

beyond the scope of claims 1-27 which are strictly limited to establishing the cryptographic key K.

Turning now to the text of the Crandall patent in column 13 at lines 18-30 cited in the Office Action, the reference states as follows.

In operation, the sender and receiver generate a common one time pad for use as an enciphering and deciphering key in a secure transmission. The private key of the sender,  $ourPri$ , is provided to the elliptic multiplier 805, along with the sender's public key,  $theirPub$ <sup>26</sup>. The elliptic multiplier 805 computes an enciphering key  $e_k$  from  $(ourPri)^o(theirPub) \pmod p$ . The enciphering key is provided to the encryption/decryption means 803, along with the plaintext message Ptxt. The enciphering key is used with an encrypting scheme, such as the DES scheme or the elliptic curve scheme of the present invention, to generate a ciphertext message C. The ciphertext message is transmitted to the receiver 802 over a nonsecure channel 816. (Emphasis supplied.)

First, Appellant observes that the preceding text describes only creating the ciphertext C and sending it to the receiver. That is, the preceding text fails to describe generating the digital signature  $(u,P)$ . Consequently, Appellant respectfully submits that the Crandall patent's text identified in the January 18, 2005, Office Action as disclosing the third characteristic step, in fact, fails to support the Office Action's allegation because the cited text fails to describe generating a digital signature  $(u,P)$ .

---

<sup>26</sup> It appears that this text should correctly read "along with the ~~sender's~~ receiver's public key,  $theirPub$ ."



Appl. No. 09/655,229  
Response Dated June 20, 2005  
Appeal of Office Action dated January 18, 2005

Presumably, the January 18, 2005, Office Action's oversight identified in the preceding paragraph might be cured by an additional citation to some text in the Crandall patent which discloses generating the digital signature (u,P). However, the problem described in detail below caused by selecting the ciphertext message C and the digital signature (u,P) to be the "plurality of sender's quantities" required by the third characteristic step is not so easily cured.

The fifth characteristic step of independent claims 1, 10 and 19 requires that at least some of the "plurality of sender's quantities" be used in computing the "cryptographic key K." If it were possible for the receiver to compute the cryptographic key K using only the ciphertext message and signature, there exists nothing to prevent an eavesdropper from similarly computing the cryptographic key K<sup>27</sup>. Thus, the preceding allegation appearing in the January 18, 2005, Office Action, if adopted, renders the Crandall patent's cryptosystem nothing more than a failed experiment because it provides totally insecure communication.

Stated in a slightly different way, both the Crandall patent's ciphertext message C and digital signature (u,P) are encrypted. If

---

<sup>27</sup> Presumably, an eavesdropper has access to:  
1. the public source 813; and  
2. everything transmitted over the nonsecure channel 816 including the ciphertext C and the digital signature (u,P).

Appl. No. 09/655,229

Response Dated June 20, 2005

Appeal of Office Action dated January 18, 2005

either or both of the ciphertext message and digital signature together with quantities available from the public source 813 permit computing the receiver's cryptographic key K as alleged in the January 18, 2005, Office Action with respect to characteristic step 5, then encrypting the message and digital signature would be futile. In a cryptosystem which truly provides confidentiality it should be extremely difficult, preferably impossible, to compute the cryptographic key K from either or both the ciphertext message and digital signature, either with or without the assistance of publicly available quantities. Thus, interpretation 3' alleged in the January 18, 2005, Office Action renders the Crandall patent's disclosure useless for its intended purpose, i.e. providing secure cryptographic communication.

Appellant respectfully submits that the January 18, 2005, Office Action's compromising security provided by the Crandall patent's cryptosystem by selecting the ciphertext message C and digital signature (u,P) to be the "plurality of sender's quantities" required by the third characteristic step of independent claims 1, 10, and 19 and the requirement of the fifth characteristic step that the "plurality of sender's quantities" be used in computing the "cryptographic key K" further demonstrates that Appellant's communications, i.e. in this instance the claims of the patent application as originally filed and/or the Crandall patent, either are not being read, or are not being understood.

Appl. No. 09/655,229

Response Dated June 20, 2005

Appeal of Office Action dated January 18, 2005

If for the preceding reason one were to reject the January 18, 2005, Office Action's allegation that the "plurality of sender's quantities" are:

1. the ciphertext message C; and
2. the digital signature (u,P);

then the only other possibility is that the Crandall patent instead discloses that, using at least some of the plurality of public quantities, the sender computes and transmits to the receiver, via the public source 813, only a single quantity, ourPub. Furthermore, in the same way as previously explained in connection with the receiver transmitting for storage in the public source 813 only a single quantity theirPub, the text of the Crandall patent expressly discloses that:

1. the sender stores only a single quantity, i.e. ourPub, into the public source 813; and
2. other quantities, i.e. the cryptosystem's parameters, are stored into the public source 813 for both sender and receiver, apparently by a trusted third party.

Using Interpretation 3 of the  
Crandall Patent, There Exists No  
Plurality of Sender's Quantities  
For Computing the Cryptographic Key K

The fifth characteristic step of independent claims 1, 10 and 19 requires that the receiving unit R use at least one of the

Appl. No. 09/655,229  
Response Dated June 20, 2005  
Appeal of Office Action dated January 18, 2005

plurality of sender's quantities received from the sending unit S in computing the cryptographic key K. However, if contrary to the January 18, 2005, Office Action's allegation:

1. the ciphertext message C; and
2. the digital signature (u,P);

are not the plurality of sender's quantities, then the only other thing which the sender computes and transmits in a way that permits access by the receiver is the sender's public quantity, i.e. ourPub. However, ourPub is a single quantity whereas the third and fifth characteristic steps of independent claims 1, 10 and 19 both require a "plurality of sender quantities." Thus, under interpretation 3 there does not exist the "plurality of sender quantities" required by independent claims 1, 10, and 19.

**A Cryptosystem's Key  
Should Be Secure**

The fifth characteristic step of independent claims 1, 10 and 19 requires that the receiving unit R use at least one of the plurality of sender's quantities received from the sending unit S in computing the cryptographic key K. If as alleged in the January 18, 2005, Office Action the plurality of sender's quantities are:

1. the ciphertext message C; and
2. the digital signature (u,P);

Appl. No. 09/655,229

Response Dated June 20, 2005

Appeal of Office Action dated January 18, 2005

and if the Crandall patent's cryptosystem truly provides confidentiality, then it is extremely difficult, preferably impossible, for the receiver to compute the cryptographic key K using at least one of the plurality of sender's quantities. In fact, if the Crandall patent's cryptosystem truly provides confidentiality then the receiver is in no better position than an eavesdropper, and, contrary to the January 18, 2005, Office Action's implicit allegation, to obtain the cryptographic key K, i.e. deciphering key  $d_K$ , the receiver must therefore crack the Crandall patent's elliptic curve cryptosystem.

Digital Signature Claims  
Are Patentable

Independent digital signature claim 28 requires that the receiver retrieve a plurality of public quantities from a publicly accessible repository which the sending unit has previously stored there. In rejecting independent claim 28 the January 18, 2005, Office Action on page 10 alleges:

the sending unit S transmits for storage in a publicly accessible repository a plurality of public quantities  
(Crandall: column 20 lines 15-24

\*

\*

\*

the receiving unit R . . . . :  
a. retrieving the plurality of public quantities from the  
publicly accessible repository (Crandall: column 17  
lines 1-50 (Emphasis supplied.)

The two texts from the Crandall patent identified above appear in the following excerpts.

A separate source 813 stores publicly known information, such as the public keys "ourPub" and "theirPub" of sender 1201 and receiver 1202, the initial point (x<sub>1</sub>, y<sub>1</sub>), the field F<sub>pk</sub>, and curve parameter "a". This source of information may be a published directory, an on-line source for use by computer systems, or it may be transmitted between sender and receiver over a non-secure transmission medium. The public source 813 is shown symbolically connected to sender 1201 through line 815 and to receiver 1202 and hasher 1206 through lines 814 and 1218 respectively. (Col. 20, lines 15-24.) (Emphasis supplied.)

\*

\*

\*

1) Using the u part of the signature, compute the point

$$Q = u^{\circ}(X_1/1)$$

2) Compare the point Q to the point

$$R = P + M(\text{ciphertext}, P)^{\circ}\text{ourPub}$$

The signature is invalid if these elliptic points Q and R do not compare exactly. In other words, if the signature is authentic, the following must hold:

$$u^{\circ}(X_1/1) = P + M(\text{ciphertext}, P)^{\circ}\text{ourPub}$$

Substituting for u on the left side of the equation above gives:

$$(m + \text{ourPri} * M(\text{ciphertext}, P))^{\circ}(X_1/1) = P + M(\text{ciphertext}, P)^{\circ}\text{ourPub}$$

or:

$$m^{\circ}(X_1/1) + (\text{ourPri} * M(\text{ciphertext}, P))^{\circ}(X_1/1) = P + M(\text{ciphertext}, P)^{\circ}\text{ourPub}$$

Substituting for ourPub on the right side of the equation yields:

$$m^{\circ}(X_1/1) + (\text{ourPri} * M(\text{ciphertext}, P))^{\circ}(X_1/1) = P + M(\text{ciphertext}, P)^{\circ}\text{ourPri}^{\circ}(X_1/1)$$

Appl. No. 09/655,229

Response Dated June 20, 2005

Appeal of Office Action dated January 18, 2005

Since  $P = m^{\circ}(X_1 / 1)$  from above, the left side becomes:

$$P + (\text{ourPri} * M(\text{ciphertext}, P))^{\circ}(X_1 / 1) = \\ P + M(\text{ciphertext}, P)^{\circ} \text{ourPri}^{\circ}(X_1 / 1)$$

Moving ourPri in the right side of the equation gives:

$$P + \text{ourPri} * M(\text{ciphertext}, P))^{\circ}(X_1 / 1) = \\ P + \text{ourPri} * M(\text{ciphertext}, P)^{\circ}(X_1 / 1)$$

Thus, a point on a curve is calculated via two different equations using the transmitted pair (u, P). It can be seen that by calculating Q from the transmitted point u, and by calculating R from transmitted point P, the ciphertext message, and the public key of the purported sender, the digital signature is assumed authenticated when Q and R match. (Col. 17, lines 1-50) (Emphasis supplied.)

Regarding the first allegation that the Crandall patent discloses a sender which stores a plurality of quantities into the public source 813, previously in this Appeal Brief it has been irrefutably established that the text of the Crandall patent expressly discloses that:

1. the sender stores only a single quantity, i.e. ourPub, into the public source 813; and
2. other quantities, i.e. the cryptosystem's parameters, are stored into the public source 813 for both sender and receiver, apparently by a trusted third party.

Neither of the Crandall patent's texts identified by the January 28, 2005, Office Action in rejecting independent claim 28 contain anything which contradicts preceding facts nos. 1 and 2.

Appl. No. 09/655,229  
Response Dated June 20, 2005  
Appeal of Office Action dated January 18, 2005

For these two reasons alone, independent digital signature claim 28, together with claim 29 depending therefrom, traverse rejection under 35 U.S.C. § 102(b) based upon the Crandall patent.

Furthermore, since for reasons nos. 1 and 2 above the sender does not store a plurality of public quantities into the Crandall patent's public source 813 as expressly required by the text of independent digital signature claim 28, the receiver cannot retrieve from the public source 813 something which the sender has not stored there. For this second reason, independent digital signature claim 28, together with claim 29 depending therefrom, traverse rejection under 35 U.S.C. § 102(b) based upon the Crandall patent.

Independent digital signature claim 28 also requires that the receiver use the digital signature, which the sending unit transmits together with message "M," and the plurality of public quantities, in evaluating expressions of at least two (2) different verification relationships. In rejecting independent claim 28 the January 18, 2005, Office Action on pages 10 and 11 alleges:

the receiving unit R . . . . :  
b. using the digital signature and the plurality of public quantities, evaluating expressions of at least two (2) different verification relationships (Crandall: column 17 lines 44-50: two different equations) (Emphasis supplied.)



Appl. No. 09/655,229  
Response Dated June 20, 2005  
Appeal of Office Action dated January 18, 2005

Lines 44-50 in the Crandall patent cited in support of the preceding allegation appear in the immediately preceding excerpt from column 17.

The text cited in the Crandall patent states that "a point on a curve is calculated via two different equations using the transmitted pair (u, P)." The text of pending independent digital signature claim 28 expressly requires:

using the digital signature and the plurality of public quantities, evaluating expressions of at least two (2) different verification relationships.

The claims of a patent, which define the invention, are "to be construed in light of the specification and both are to be read with a view to ascertaining the invention." United States v. Adams, 383 U.S. 39, 49, 148 USPQ 479, 482 (1966). (Emphasis supplied) In the terminology of the present application beginning on page 22 at line 14, computing the points Q and R constitutes evaluating expressions of a single verification relationship. Expressing the Crandall patent's disclosure in the terminology of the present application produces the following verification relationship.

$$u^{\circ}(X_1/1) = Q \neq R = P + M(\text{ciphertext}, P)^{\circ}\text{ourPub}$$

Appl. No. 09/655,229  
Response Dated June 20, 2005  
Appeal of Office Action dated January 18, 2005

The preceding verification relationship, which corresponds to the Crandall patent's disclosure in column 17, lines 1-50, requires evaluating only the two (2) following expressions.

$$u^{\circ}(X_1 / 1)$$

$$P + M(\text{ciphertext}, P)^{\circ}\text{ourPub}$$

For this third reason, independent digital signature claim 28, together with claim 29 depending therefrom, traverse rejection under 35 U.S.C. § 102(b) based upon the Crandall patent.

Independent digital signature claim 28 further requires that the receiver compare pairs of results obtained by evaluating the expressions of the at least two (2) different verification relationships. In rejecting independent claim 28 the January 18, 2005, Office Action on pages 10 and 11 alleges:

the receiving unit R . . . . :  
c. comparing pairs, of results obtained by evaluating the expressions of the at least two (2) different verification relationships (Crandall: column 17 lines 49-50: the digital signature is assumed authenticated when Q and R match) (Emphasis supplied.)

Lines 49-50 in the Crandall patent cited in support of the preceding allegation appear in the immediately preceding excerpt from column 17.

The text cited in the Crandall patent states that "the digital signature is assumed authenticated when Q and R match." The text of pending independent digital signature claim 28 expressly requires:

Appl. No. 09/655,229  
 Response Dated June 20, 2005  
 Appeal of Office Action dated January 18, 2005

comparing pairs of results obtained by evaluating the expressions of the at least two (2) different verification relationships.

Note first that the text of independent claim 28 requires "comparing pairs of results . . . ." Thus, the text of independent claim 28 expressly requires comparing more than the single pair of results Q and R disclosed in the Crandall patent.

Set forth below are the two verification relationships which appear in the present application on page 22 at line 19-22 recast to use the terminology of the Crandall patent.

$$1. \quad m^{(((a \cdot p)^n) a + a \times p) \cdot a \times (a \times a)} = Q_1$$

$$\neq R_1 = m^{a \times (a \times (a \times a)) \cdot p}$$

$$2. \quad m^{(((a \cdot p)^n) a + a \times p) \cdot (a \times (a \times a)) \times a} = Q_2$$

$$\neq R_2 = m^{-(a \cdot a) \cdot a \times (a \times a) \cdot p}$$

Clearly, the single "verification relationship" disclosed in the Crandall patent set forth above cannot anticipate the two (2) verification relationships disclosed in the present application and encompassed by independent digital signature claim 28. For this fourth reason, independent digital signature claim 28, together with claim 29 depending therefrom, traverse rejection under 35 U.S.C. § 102(b) based upon the Crandall patent.

Conclusion

The text of the Crandall patent expressly discloses that:

1. the receiver stores only a single quantity, i.e. theirPub, into the public source 813<sup>28</sup>;
2. the sender stores only a single quantity, i.e. ourPub, into the public source 813<sup>29</sup>; and
3. other quantities, i.e. the Crandall patent cryptosystem's parameters, are not stored into the public source 813 by either the receiver or the sender, but are rather stored for both sender and receiver, apparently by a trusted third party<sup>30</sup>.

Since independent cryptographic key K claims 1, 10 and 19, together with all claims depending therefrom, stand finally rejected as being anticipated under 35 U.S.C. § 102(b) by the Crandall patent, for reasons set forth above claims 1-27 traverse the rejection based solely upon facts nos. 1 and 3 above.

Since independent digital signature claim 28 and claim 29 depending therefrom stand finally rejected as being anticipated

---

<sup>28</sup> See the Crandall patent at col. 8, lines 8-23.

<sup>29</sup> Id.

<sup>30</sup> See the Crandall patent:  
1. col. 7, lines 30-31 which expressly states that "parameters are established for both sender and recipient" (receiver); and  
2. col. 16, lines 15-24.

Appl. No. 09/655,229

Response Dated June 20, 2005

Appeal of Office Action dated January 18, 2005

under 35 U.S.C. § 102(b) by the Crandall patent, for reasons set forth above claims 28 and 29 traverse the rejection based solely upon facts nos. 2 and 3 above.

Furthermore, for reasons explained in greater detail above independent cryptographic key K claims 1, 10 and 19, together with all claims depending therefrom, also traverse rejection under 35 U.S.C. § 102(b) because the Crandall patent also:

1. either:

- a. fails to disclose the sending unit S using at least some of the plurality of public quantities in computing and transmitting to the receiving unit R a plurality of sender's quantities; or
- b. relies upon portions of the Crandall patent's disclosure lying beyond the scope of the pending claims which encompass only establishing a cryptographic key K; and

2. either:

- a. fails to disclose the receiving unit R using at least one of the plurality of sender's quantities received from the sending unit S in computing the cryptographic key K; or
- b. discloses a cryptosystem that provides no security.

Furthermore, for reasons explained in greater detail above independent digital signature claim 28 and claim 29 depending therefrom traverse rejection under 35 U.S.C. § 102(b) because the Crandall patent also fails to disclose:

Appl. No. 09/655,229

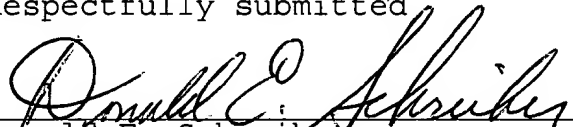
Response Dated June 20, 2005

Appeal of Office Action dated January 18, 2005

1. the receiver retrieving from the public source 813 a plurality of quantities which the sender has stored there;
2. the receiver evaluating expressions of at least two (2) different verification relationships; and
3. comparing pairs of results obtained by evaluating the expressions of the at least two (2) different verification relationships.

For all the various reasons set forth above, the Board of Appeal must overrule the rejections of claims 1-29 appearing in the Examiner's Action dated January 18, 2005, and order that this application pass to issue.

Respectfully submitted



Donald E. Schreiber

Reg. No. 29,435

Dated: 20 June, 2005

Donald E. Schreiber  
A Professional Corporation  
Post Office Box 2926  
Kings Beach, CA 96143-2926

Telephone: (530) 546-6041

Attorney for Appellant

**APPENDIX I**  
**CLAIMS**

1. In a protocol for cryptographic communication via a communication channel "I" in which a sending cryptographic unit "S" transmits onto the communication channel I an encrypted cyphertext message "M" obtained by supplying both a plaintext
- 5 message "P" and a cryptographic key "K" to a first cryptographic device, and in which a receiving cryptographic unit "R" receives the cyphertext message M from the communication channel I and by supplying the cyphertext message M together with the key K to a second cryptographic device decrypts the plaintext message P
- 10 therefrom, a method by which the units S and R mutually establish a cryptographic key K by first exchanging messages before the sending unit S transmits the cyphertext message M comprising the steps of:
- a. the receiving unit R transmitting for storage in a

15 publicly accessible repository a plurality of public quantities;

  - b. the sending unit S:
    - i. retrieving the plurality of public quantities from the publicly accessible repository;

20 ii. using at least some of the plurality of public quantities, computing and transmitting to the receiving unit R a plurality of sender's quantities; and

- 25                   iii. using at least one of the plurality of public  
                    quantities, computing the key K; and
- c.    the receiving unit R, using at least one of the plural-  
            ity of sender's quantities received from the sending  
            unit S computing the key K.

2.    The method of claim 1 wherein the receiving unit R, in  
storing the plurality of public quantities into the publicly  
accessible repository:

- 5           i.    selects at least one receiver's secret quantity;
- ii.   selects for storage in the publicly accessible  
                repository as part of the plurality of public  
                quantities at least one selected public quantity;  
                and
- 10          iii. using the receiver's secret quantity and the at  
                least one selected public quantity, computes and  
                stores in the publicly accessible repository as  
                part of the plurality of public quantities a plu-  
                rality of computed public quantities.

3.    The method of claim 2 wherein the plurality of public  
quantities include a plurality of vectors.



4. The method of claim 2 wherein the at least one selected public quantity includes a vector.

5. The method of claim 2 wherein the plurality of computed public quantities include a plurality of vectors.

6. The method of claim 2 wherein the sending unit S, in computing the plurality of sender's quantities for transmission to the receiving unit R:

- i. selects a sender's secret quantity; and
- 5 ii. using the sender's secret quantity and at least some of the retrieved plurality of public quantities, computes for transmission to the receiving unit R the plurality of sender's quantities.

7. The method of claim 6 wherein the plurality of sender's quantities include a plurality of vectors.

8. The method of claim 1 wherein the sending unit S, in computing the plurality of sender's quantities for transmission to the receiving unit R:

- i. selects a sender's secret quantity; and

- 5           ii. using the sender's secret quantity and at least  
            some of the retrieved plurality of public quantities,  
            computes for transmission to the receiving  
            unit R the plurality of sender's quantities.

9. The method of claim 8 wherein the plurality of sender's quantities include a plurality of vectors.

10. A system adapted for communicating as an encrypted cyphertext message M a plaintext message P that has been encoded using a cryptographic key K, the system comprising:

- 5           a. a communication channel I adapted for transmitting the  
            cyphertext message M;
- b. a pair of transceivers that are coupled to said communication channel I, and that are adapted for communicating the cyphertext message M from one transceiver to the other transceiver via said communication channel I;
- 10           and
- c. a pair of cryptographic units each of which is respectively coupled to one of said transceivers for transmitting the cyphertext message M thereto or receiving the cyphertext message M therefrom, each cryptographic
- 15           unit:

i. when the cryptographic unit is to receive the  
cyphertext message M:

(1) storing plurality of public quantities in a  
publicly accessible repository;

20 (2) receiving via the communication channel I a  
plurality of sender's quantities from a send-  
ing cryptographic unit, and using at least  
one of the plurality of sender's quantities  
in computing the key K; and

25 ii. when the cryptographic unit is to send the  
cyphertext message M, retrieving the plurality of  
public quantities from the publicly accessible  
repository and using:

30 (1) at least some of the plurality of public  
quantities in computing the plurality of  
sender's quantities which the sending crypto-  
graphic unit transmits via the communication  
channel I to the receiving cryptographic  
unit; and

35 (2) at least one of the plurality of public quan-  
tities in computing the key K; and

iii. including a cryptographic device having:

- (1) a key input port for receiving the key K from the cryptographic unit;
- 40 (2) a plaintext port:
  - (a) for accepting the plaintext message P for encryption into the cyphertext message M that is transmitted from the cryptographic device, and
  - 45 (b) for delivering the plaintext message P obtained by decrypting the cyphertext message M received by the cryptographic device; and
- 50 (3) a cyphertext port that is coupled to one of said transceivers:
  - (a) for transmitting the cyphertext message M to such transceiver, and
  - (b) for receiving the cyphertext message M from such transceiver.

11. The system of claim 10 wherein said cryptographic unit which receives the cyphertext message M in storing the plurality of public quantities into the publicly accessible repository:

- (a) selects at least one receiver's secret quantity;

- 5                   (b) selects for storage in the publicly accessible repository as part of the plurality of public quantities at least one selected public quantity; and
- 10                   (c) using the receiver's secret quantity and the at least one selected public quantity, computes and stores in the publicly accessible repository as part of the plurality of public quantities a plurality of computed public quantities.

12. The system of claim 11 wherein the plurality of public quantities include a plurality of vectors.

13. The system of claim 11 wherein the at least one selected public quantity includes a vector.

14. The system of claim 11 wherein the plurality of computed public quantities include a plurality of vectors.

15. The system of claim 11 wherein the sending cryptographic unit, in computing the plurality of sender's quantities for transmission to the receiving cryptographic unit::

- i. selects a sender's secret quantity;; and

- 5           ii. using the sender's secret quantity and at least some of the retrieved plurality of public quantities, computes for transmission to the receiving cryptographic unit the plurality of sender's quantities.

16. The system of claim 15 wherein the plurality of sender's quantities include a plurality of vectors.

17. The system of claim 10 wherein the sending cryptographic unit, in computing the plurality of sender's quantities for transmission to the receiving cryptographic unit:

- 5           i. selects a sender's secret quantity;; and  
          ii. using the sender's secret quantity and at least some of the retrieved plurality of public quantities, computes for transmission to the receiving cryptographic unit the plurality of sender's quantities.

18. The system of claim 17 wherein the plurality of sender's quantities include a plurality of vectors.

19. A cryptographic unit adapted for inclusion in a system for communicating as an encrypted cyphertext message M a plaintext message P that has been encoded using a cryptographic key K, the system including:

- 5           a. a communication channel I adapted for transmitting the cyphertext message M; and
- b. a pair of transceivers that are coupled to said communication channel I, and that are adapted for communicating the cyphertext message M from one transceiver to
- 10           the other transceiver via said communication channel I; the cryptographic unit being adapted for coupling to said transceivers for transmitting the cyphertext message M thereto or receiving the cyphertext message M therefrom, and comprising:
  - a. ports:
    - 15           i. when the cryptographic unit is to receive the cyphertext message M, for:
      - (1) storing plurality of public quantities in a publicly accessible repository;
      - (2) receiving via the communication channel I a
      - 20           plurality of sender's quantities from a sending cryptographic unit, and using at least one of the plurality of sender's quantities in computing the key K; and

ii. when the cryptographic unit is to send the  
25 cyphertext message M, for retrieving the plurality  
of public quantities from the publicly accessible  
repository and using:

(1) at least some of the plurality of public  
quantities in computing the plurality of  
30 sender's quantities which the sending crypto-  
graphic unit transmits via the communication  
channel I to the receiving cryptographic  
unit; and

(2) at least one of the plurality of public quan-  
35 tities in computing the key K; and

b. a cryptographic device having:

i. a key input port for receiving the key K from the  
cryptographic unit;

ii. a plaintext port:

(1) for accepting the plaintext message P for  
40 encryption into the cyphertext message M that  
is transmitted from the cryptographic device,  
and

(2) for delivering the plaintext message P ob-  
45 tained by decrypting the cyphertext message M  
received by the cryptographic device; and



ii. a cyphertext port that is coupled to one of said transceivers:

- (1) for transmitting the cyphertext message M to such transceiver, and
- (2) for receiving the cyphertext message M from such transceiver.

50

20. The cryptographic unit of claim 19 wherein, when receiving the cyphertext message M, in storing the plurality of public quantities into the publicly accessible repository:

- (a) selects at least one receiver's secret quantity;
- (b) selects for storage in the publicly accessible repository as part of the plurality of public quantities at least one selected public quantity; and
- (c) using the receiver's secret quantity and the at least one selected public quantity, computes and stores in the publicly accessible repository as part of the plurality of public quantities a plurality of computed public quantities.

5

10

21. The cryptographic unit of claim 20 wherein the plurality of public quantities include a plurality of vectors.

22. The cryptographic unit of claim 20 wherein the at least one selected public quantity includes a vector.

23. The cryptographic unit of claim 20 wherein the plurality of computed public quantities include a plurality of vectors.

24. The cryptographic unit of claim 20, when sending the cyphertext message M, in computing the plurality of sender's quantities for transmission to the receiving cryptographic unit:

- i. selects a sender's secret quantity; and
- 5 ii. using the sender's secret quantity and at least some of the retrieved plurality of public quantities, computes for transmission to the receiving cryptographic unit the plurality of sender's quantities.

25. The cryptographic unit of claim 24 wherein the plurality of sender's quantities include a plurality of vectors.

26. The cryptographic unit of claim 19 wherein, when sending the cyphertext message M, in computing the plurality of

Appl. No. 09/655,229

Response Dated June 18, 2005

Appeal of Office Action dated January 18, 2005

sender's quantities for transmission to the receiving cryptographic unit:

- 5           i.    selects a sender's secret quantity; and
- ii.   using the sender's secret quantity and at least  
              some of the retrieved plurality of public quantities, computes for transmission to the receiving  
              cryptographic unit the plurality of sender's quantities.
- 10

27. The cryptographic unit of claim 26 wherein the plurality of sender's quantities include a plurality of vectors.

28. In a protocol for communication in which a sending unit S transmits onto the communication channel I a message "M" together with a digital signature, and, wherein before transmitting the message M and the digital signature, the sending unit S
- 5   transmits for storage in a publicly accessible repository a plurality of public quantities, a method by which a receiving unit R that receives the message M and the digital signature verifies the authenticity of digital signature comprising the steps performed by the receiving unit R of:
- 10       a.    retrieving the plurality of public quantities from the publicly accessible repository;

Appl. No. 09/655,229

Response Dated June 18, 2005

Appeal of Office Action dated January 18, 2005

b. using the digital signature and the plurality of public quantities, evaluating expressions of at least two (2) different verification relationships; and

15 c. comparing pairs of results obtained by evaluating the expressions of the at least two (2) different verification relationships.

29. The method of claim 28 wherein the plurality of public quantities include a plurality of vectors.